UNITED STATES DISTRICT COURT

for the

District of New Hampshire

SEALED DOCUMENT

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE PREMISES LOCATED AT 108 HOWARD ST, APT 2, KEENE, NH, A GRAY NISSAN SENTRA NH 4833590, AND THE PERSON OF JASON RIDDLE

Case No. 1:21-mj- 16-01/03-AJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see attachment A.

located in the _____ District of New Hampshire, there is now concealed *(identify the person or describe the property to be seized)*:

Please see attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
PLEASE SEE ATTACHMENT OF OFFENSES	

The application is based on these facts:

Please see attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Shayne Tongbua
Applicant's signature

S.A. Shayne Tongbua, Federal Bureau of Investigation
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephonic conference *(specify reliable electronic means).*

Date: 01/20/2021

Andrea K. Johnstone
Judge's signature

City and state: Concord, New Hampshire

Hon. Andrea K. Johnstone, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT 108 HOWARD ST, APT 2, KEENE, NH, A GRAY NISSAN SENTRA NH 4833590, AND THE PERSON OF JASON RIDDLE	Case No. 1:21-mj-_____ **Filed Under Seal – Level II**

CODE SECTIONS AND OFFENSE DESCRIPTIONS CONTINUED FROM WARRANT APPLICATION

1. 18 U.S.C. §§ 231(a)(3) – Certain Acts During Civil Disorder
2. 18 U.S.C. § 1752(a) – Unlawful Entry
3. 18 U.S.C. § 2101 – Travel with Intent to Riot
4. 18 U.S.C. § 641 – Theft of Government Property
5. 40 U.S.C. § 5104(e)(2) – Unlawful Activity in the Capitol

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT 108 HOWARD ST, APT 2, KEENE, NH, A GRAY NISSAN SENTRA NH 4833590, AND THE PERSON OF JASON RIDDLE	Case No. 1:21-mj-_____ **Filed Under Seal – Level II**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Shayne Tongbua, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been employed with the FBI since 2009. In the course of my duties, I have investigated and supported operations involving national security matters relating to economic espionage and terrorism, as well as federal criminal violations concerning crimes against children, human-trafficking, narcotics, organized crime, international and domestic terrorism, weapons of mass destruction, and other criminal violations. I have acquired experience in investigating various violations of federal law through extensive training at the FBI Academy in Quantico, Virginia, and by conducting investigations in the field. During my career, I have participated in many criminal investigations as a case agent and/or in a subsidiary role and have participated in the execution of numerous federal search warrants. Prior to becoming an FBI Special Agent, I also served as an Information Technology Specialist – Forensic Examiner. My duties in that capacity included extraction, preservation, and analysis of digital evidence, as well as comprehensive technical analysis of computers, mobile phones, digital media, and related equipment. Prior to joining the FBI, I also served in the US Army from 2003-2009.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located 108 Howard St, Apt 2, Keene, NH (hereafter SUBJECT PREMISES); a gray Nissan Sentra with New Hampshire Registration 4833590; and the person of Jason Riddle (RIDDLE); and any computer, computer media, and electronic media located therein or thereon; for the things described in Attachment B – specifically, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 231(a)(3), 1752(a), 2101, and 641 and 40 U.S.C. § 5104(e)(2).

3. Title 18 U.S.C. § 231(a)(3) makes it a crime to commit or attempt to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays or adversely affects commerce or the movement or of any article or commodity in commerce or the conduct or performance of any federally protected function. Civil disorder is defined as any public disturbances involving acts of violence by assemblages of three or more persons, which causes an immediate danger or injury to the property or person of any other individual. 18 U.S.C. § 232(1).

4. Title 18 U.S.C. § 1752(a) makes it a crime to (1) knowingly enter or remain in any restricted building or grounds without lawful authority to do; or (2) knowingly, and with intent to impede or disrupt the orderly conduct of Government business or official functions, engage in disorderly or disruptive conduct in, or within such proximity to, any restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of Government business or official functions. For purposes of Section 1752 of Title 18, a restricted building includes a posted, cordoned off, or otherwise restricted area of a building or grounds where the President or other person protected by the Secret Service is or will be temporarily

visiting; or any building or grounds so restricted in conjunction with an event designated as a special event of national significance.

5. Title 18 U.S.C. § 2101 prohibits travel in interstate or foreign commerce or use of any facility of interstate or foreign commerce with intent to incite a riot, organize promote, encourage, participate in, or carry on a riot, commit any act of violence in furtherance of a riot or aid or abet any person inciting or participating in or carrying on a riot or committing any act of violence in furtherance of a riot.

6. A person violates Title 18 U.S.C. § 641 if he steals . . . or knowingly converts to his use or the use of another, or without authority, sells conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency.

7. Title 40 U.S.C. § 5104(e)(2), makes it a crime for an individual or group of individuals to willfully and knowingly (D) utter loud, threatening, or abusive language, or engage in disorderly or disruptive conduct, at any place in the Grounds or in any of the Capitol Buildings with the intent to impede, disrupt, or disturb the orderly conduct of a session of Congress or either House of Congress, or the orderly conduct in that building of a hearing before, or any deliberations of, a committee of Congress or either House of Congress; or (G) parade, demonstrate, or picket in any of the Capitol Buildings.

8. During the course of this investigation I have conferred with other investigators who have conducted investigations and executed search and arrest warrants related to these offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set

forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and records related to this investigation, and information gained through my training and experience.

PROBABLE CAUSE

9. The U.S. Capitol, which is located at First Street, SE, in Washington, D.C., is secured 24 hours a day by U.S. Capitol Police. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by U.S. Capitol Police. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

10. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

11. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol, in Washington, D.C. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which had taken place on November 3, 2020. The joint session began at approximately 1:00 p.m. Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

12. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the

exterior of the U.S. Capitol building, and U.S. Capitol Police were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

13. At approximately 2:00 p.m., certain individuals in the crowd forced their way through, up, and over the barricades, and officers of the U.S. Capitol Police, and the crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials.

14. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of the U.S. Capitol Police attempted to maintain order and keep the crowd from entering the Capitol; however, shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of the U.S. Capitol Police, as others in the crowd encouraged and assisted those acts.

15. Shortly thereafter, at approximately 2:20 p.m., members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to – and did – evacuate the chambers. Accordingly, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons checks, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol,

and the building had been confirmed secured. Vice President Pence remained in the U.S. Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

16. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

17. RIDDLE was one of the individuals who entered the U.S. Capitol building with the crowd that day. RIDDLE provided an interview to NBC10 Boston News during which he discussed what he did and saw that day. According to his televised statement, he saw people who "just broke into the building" referring to the U.S. Capitol. He then went inside the Capitol and observed rioters, "smashing computers, printers, breaking things, throwing papers and lamps around." He told the newscaster that he poured himself a glass of wine that he found in a liquor cabinet inside a lawmaker's office inside the Capitol and "chugged it and got out of there." He also described those he saw committing violent acts, stating, "[t]hose psychopaths going around breaking things and hurting people can rot in hell."

18. RIDDLE provided photos and videos of the events that day to NBC10 News. According to the reporter who spoke with him, RIDDLE took the videos himself. Some of the video footage depicted a group of protestors outside the U.S. Capitol. RIDDLE also apparently provided NBC10 News with a photograph of himself inside a lawmaker's office, holding the bottle of wine he took.

19. Investigators reviewed video footage and images taken from the Capitol that day. Some of those images capture RIDDLE walking up the steps toward the entrance to the Capitol and taking photographs with his cell phone outside the Capitol apparently before entry. At that

time, he appears to be holding only a cell phone and wearing what appears to be only a small fanny pack around his waist. At a time that seems consistent with RIDDLE having exited the Capitol, he appears on video again, this time, for the first time, holding a book, depicted in the image below. The book appears too large for him to have been able to put in his fanny pack and was not seen in the images of RIDDLE before he entered the Capitol, although it is possible that it was underneath his jacket and not visible. However, based on the images, I believe it is likely that RIDDLE may have taken the book from inside the Capitol. These images also show an item resembling a cell phone in RIDDLE's front pocket.

20. Based on my review of the video and photographs shown on NBC10 News, it appears that the images were taken on a cellular telephone and therefore I believe that cellular telephones used by RIDDLE may contain evidence of the target offenses in photo/video format or otherwise. I also know that many of the protesters who entered the U.S. Capitol communicated with each other before, during, and after the protests by phone, text message and through social media or other chat applications, and that many made plans relating to their activities that day. Therefore, I believe that evidence of the identity and actions of others who entered the U.S. Capitol with RIDDLE may be found in the contacts, call logs, text messages,

and messaging applications on his cellular telephones. I also believe that evidence of RIDDLE's travel to the District of Columbia may be found on his cell phone or computers in the form of plane, bus, or train tickets, hotel reservations, internet searches, or otherwise.

I know, based on my training and experience, that cell phone users frequently use computers and other linked electronic devices to back up the content of their cellular phones including videos, photographs, communications, contacts, and more. I also know that content that has been deleted from cell phones may be available on computers or other electronic devices containing backup copies of the phone data. I know, based on my training and experience, that these items are frequently stored in people's primary residences. Additionally, in my training and experience, individuals most commonly keep their most frequently used electronic devices such as mobile phones on their person. Such devices are often attached via armbands or belt holsters, or stored in pockets of pants or coats, backpacks, purses, or other areas within arm's reach for easy access or close enough to receive notifications, whether audible or vibratory

21. The SUBJECT PREMISES is RIDDLE's registered address, located at 108 Howard St, Apt 2, Keene, NH. According to USPS records, RIDDLE's spouse is Robert SHOEN. It is unconfirmed if SHOEN currently resides at the SUBJECT PREMISES.

22. Physical surveillance conducted by law enforcement on 1/13/21 and 1/15/21 confirmed the presence of a gray, Nissan Sentra [NH 4833590] registered to RIDDLE in the vicinity of 108 Howard St in Keene, NH, the location of the SUBJECT PREMISES. In my training and experience, individuals often store frequently used electronic devices such as mobile phones and removable storage media in their vehicles. This occurrence is increasingly amplified by the multi-functionality of such devices which also serve as a primary means of navigation, communication, and multimedia / music storage. Individuals who travel frequently or have

traveled recently, often leave their mobile devices in their vehicles regularly, where they have designated accessories such as mounts or holders, Bluetooth adapters, and chargers for them.

COMPUTER ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES, including data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, iPads or tablets, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through

technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

25. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES accessible by RIDDLE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what

tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence

may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

26. Based on my training and experience I know some of the devices referenced above, which may contain evidence of crime, are by their very nature portable. This includes as example but is not limited to laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such devices in multiple locations within their premises, including in outbuildings, vehicles and/or on their person.

27. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The nature of evidence.** As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain

evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. **The volume of evidence**. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. **Technical requirements**. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. **Variety of forms of electronic media.** Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

29. This warrant seeks authorization for law enforcement to compel Jason Riddle to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

30. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

31. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly.

32. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

33. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

34. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

35. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

36. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

37. In light of the foregoing, and with respect to (1) any device found on the person of Jason RIDDLE, or (2) any device at/on the SUBJECT PREMISES and vehicle reasonably believed to be owned, used, or accessed by RIDDLE, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of RIDDLE to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of RIDDLE and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of RIDDLE and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

38. The proposed warrant does not authorize law enforcement to compel that an individual present at the SUBJECT PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the SUBJECT PREMISES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

39. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. §§ 231(a)(3), 1752(a), 2101, and 641 and 40 U.S.C. § 5104(e)(2) may be located at the SUBJECT PREMISES, in the subject vehicle, and on the person of Jason RIDDLE. I therefore seek a warrant to search the premises described in Attachment A and any computer and electronic media located therein, and to seize the items described in Attachment B.

40. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Dated: January 20, 2021

Respectfully Submitted,

/s/ Shayne Tongbua
Shayne Tongbua
Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

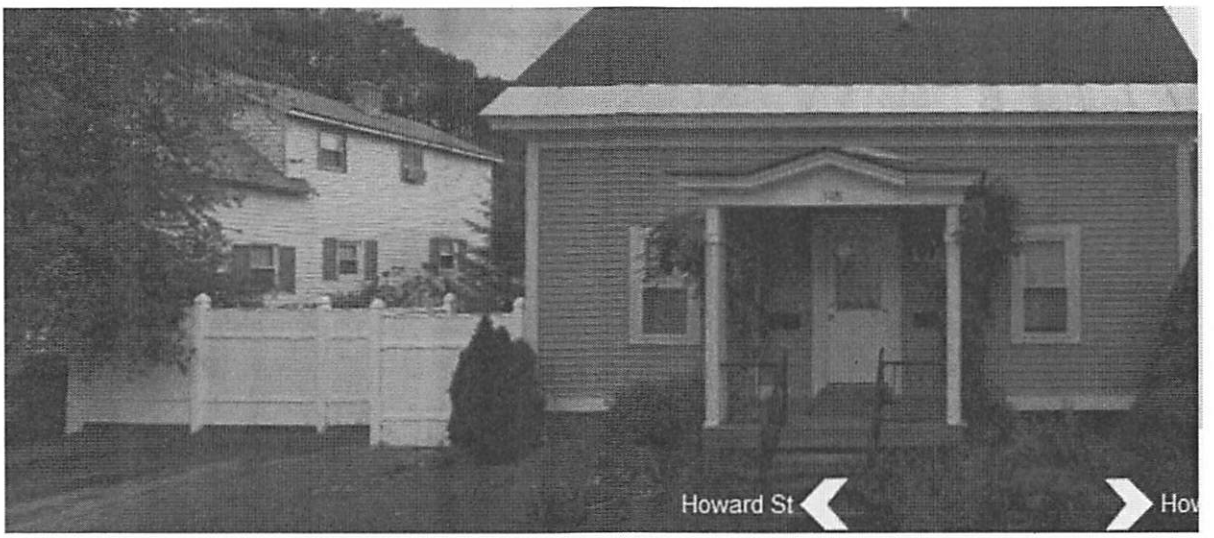
Andrea K. Johnstone

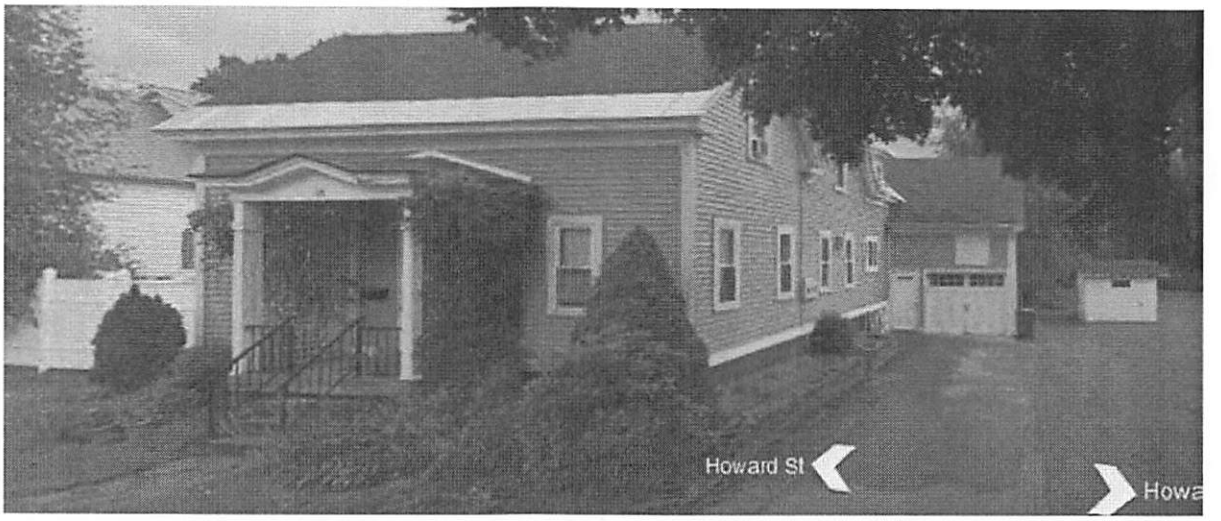
Hon. Andrea K. Johnstone
United States Magistrate Judge
Dated: January 20, 2021

ATTACHMENT A
PREMISES TO BE SEARCHED

I. Residence

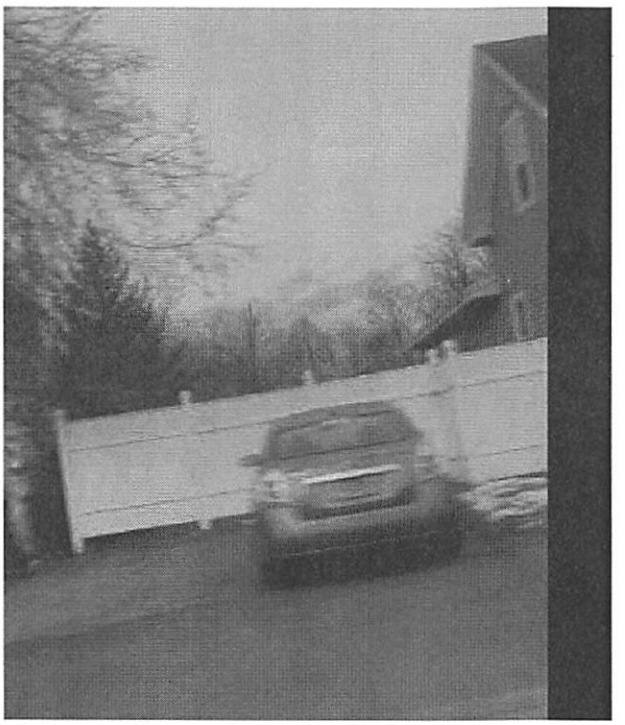
The property to be searched is 108 Howard St, Apt 2, Keene, NH 03431, identified as the residence of Jason Riddle. The primary structure is a two-story, beige/light brown, multi-unit building with light shutters and a darker brown/red roof, as well as a right side driveway and small parking area on the left in front of a white fence, both accessible from Howard St. The front door is clearly labeled 108. The property contains a garage and detached shed. The driveway is accessible from Howard St. Also to be searched on the property is any common storage area in the basement, garage, and detached shed which is accessible by all tenants, including Riddle.





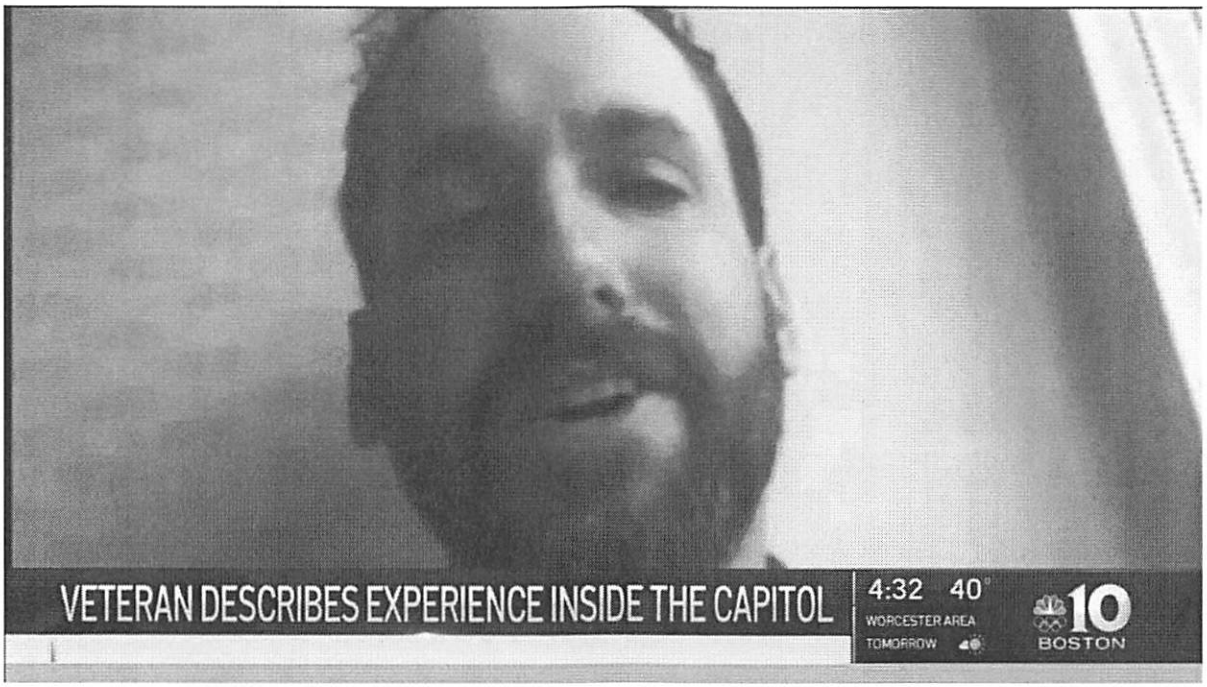
II. Vehicle

The property to be searched is a gray Nissan Sentra bearing license plate [NH 4833590]. The vehicle is registered to Jason RIDDLE. The vehicle has been observed parked at RIDDLE's known residence, as described above, located at 108 Howard St, Keene, NH.



III. Person

The area to be searched is the physical person of Jason RIDDLE, depicted in the attached photographs.



ATTACHMENT B
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 231(a)(3), 1752(a), 2101, and 641 and 40 U.S.C. § 5104(e)(2) including any computer, cellular telephone, or electronic media that were or may have been used by Jason RIDDLE as a means to commit the offenses or which may contain evidence of the offenses described on the warrant

i. photos, videos and other images of RIDDLE and others in Washington D.C. before, during and after entry of the U.S. Capitol on January 6, 2021;

ii. evidence of travel to Washington D.C. by RIDDLE and others during the week of January 6, 2021;

iii. A book consistent with the one depicted in the photograph of RIDDLE leaving the Capitol on January 6, 2021 or other items that were taken from inside the Capitol;

iv. Information identifying others present in the U.S. Capitol on January 6, 2021.

For any computer, cellular telephone, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the intentional elimination of records or information relating to violations of the statutes described above;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER'S Internet activity, including firewall logs, caches, browser history and cookies, "bookmarks" or "favorite" web pages, search terms the user entered into any Internet search engine, and records of user-typed web addresses, as relating to violations of the statutes described above;

m. contextual information necessary to understand the evidence described in this attachment; and

n. evidence of the crimes described above including but not limited to:

i. Photos, videos and other images of RIDDLE and others in Washington D.C. before, during and after entry of the U.S. Capitol on January 6, 2021;

ii. Evidence of travel to Washington D.C. by RIDDLE and others during the week of January 6, 2021;

iii. Discussions between RIDDLE and others of the entry into the U.S. Capitol on January 6, 2021 and related protests;

iv. Evidence of possession of the wine RIDDLE drank, the book, the photograph of which is included in the affidavit above, or other items taken from the U.S. Capitol on January 6, 2021;

v. Information identifying others present in the U.S. Capitol on January 6, 2021.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); and any photographic form (such as prints or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disk drives (HDD), solid-state drives (SSD), random-access memory (RAM), flash memory, memory cards, CDs, DVDs, and other magnetic or optical media.

DEVICE UNLOCK: During the execution of the search of the property described in Attachment A, and with respect to (1) any device on Jason RIDDLE's person, or (2) any device at/on SUBJECT PREMISES or vehicle reasonably believed to be owned, used, or accessed by RIDDLE, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of RIDDLE to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of RIDDLE and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of that RIDDLE and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.